EL DINAR: Jurnal Keuangan dan Perbankan Syariah
Volume 14, No 1 (2026)
E ISSN: 2622-0083

FROM CYBER DISRUPTION TO DIGITAL TRUST: THE MEDIATING ROLE OF RELIGIOSITY IN ISLAMIC BANKING

Harun Alrasyid, Dinda Dwi Nurrizkiana

Faculty of Economy and Business, Universitas Islam Malang
MT. Haryono Street No. 193, Malang, East Jawa, 65144, Indonesia

✉ Corresponding Author:
Author's name: Harun Alrasyid
E-mail: harunalrasyid@unisma.ac.id

Abstract

The present study investigates the interplay among trust, perceived security, risk management, and reputation in the context of a cyber-incident in Islamic banking services with religiosity as a mediator. The respondents consisted of 247 Indonesian customers of Islamic banks. PLS-SEM was used to analyze the collected data. The results revealed that religiosity strongly increases the level of trust and mediates the impact of perceived security and reputation. Meanwhile, risk management impacts trust directly. Reputation did not affect the target construct directly, yet had a highly mediated impact on trust through religiosity, suggesting that in a crisis situation, institutional credibility is mainly evaluated through the religious perspective. The present results indicates that the restoration of digital trust in post cyber-incident should be based not only on technical aspects (effective security and risk management) but also on value-based aspects according to the Shariah law. Islamic banks should focus their efforts on communicating cybersecurity measures and practices as part of their ethical responsibility, emphasize accountability and the protection of stakeholders' rights, and work together with religious institutions to build up their credibility. This study contributes to Commitment–Trust Theory, as it reveals that religiosity can be considered an evaluation process in translating institutional practices into trust.

Keywords: Islamic Banking; Customer Trust; Cybersecurity; Religiosity; Risk Management

INTRODUCTION

As the utilization of digital platforms in Islamic banking continues to grow, more Islamic banks have leveraged technology to ensure accessibility and effectiveness in providing Sharia-compliant banking services (Zouari & Abdelhedi, 2021). Nonetheless, the adoption of these technologies presents an opportunity for cyber-attacks, which can affect the provision of these services and damage customers' trust in these institutions (Jafri et al., 2024; Susanti et

al., 2023). The growing use of digital platforms implies that more clients rely on the security of their information, which, when violated by cybercriminals, poses a threat to their privacy and the overall reputation of the Islamic banks. Thus, cybersecurity cannot be ignored anymore since it is now not only a technical issue but also a strategy that has a direct impact on the credibility of an institution. The problem that arises for Islamic banks is how to maintain their technological capabilities without compromising their trust built on religious and ethical values.

Cyber threats facing Islamic banks can be further demonstrated through recent examples from Islamic financial institutions, which show the gravity of such cyber threats on the institution's trust. In May 2023, one of Indonesia's biggest Islamic banks suffered from service disruption that lasted for a few days. After investigation, the financial regulatory authority stated that services were available again since 13 May 2023 (OJK, 2023). On the other hand, an independent report stated that there was ransomware involved in the attack, and LockBit claimed data exfiltration and threatened to publish around 1.5 TB of data from the bank (Kholis, 2025; Ramadhanu et al., 2025; Sulubara, 2024). Such events clearly showcase that a cyber incident can affect both the availability of services and information security of the bank's customers at once. Due to this, customers are likely to lose trust in Islamic banks because of both issues.

These disruptions have significant implications for customer perceptions and behavior. Service outages restrict access to accounts and financial transactions, while concerns over data breaches raise doubts about institutional reliability and security (Hossain et al., 2025; Jafri et al., 2024). In this context, cyber resilience becomes essential, referring to the ability of financial institutions to anticipate, withstand, and recover from cyber incidents while maintaining critical operations (Elansari et al., 2024). Cyber threats also extend beyond technical vulnerabilities, encompassing perceived security risks, governance challenges, and reputational consequences (Shehab et al., 2024). While conventional banks primarily rely on technical recovery to restore trust, Islamic banks face additional expectations. They must demonstrate not only operational competence but also adherence to ethical and religious principles, ensuring that no violation of Sharia values has occurred (Muflih et al., 2024; Usman et al., 2017). This dual requirement makes trust restoration in Islamic banking more complex and multidimensional.

Trust in financial service organizations is a multidimensional construct, comprising elements of competence, integrity, and benevolence Gefen et al. (2003) and Morgan & Hunt (1994). In online banking services, competence

pertains to security and risk management skills, while integrity concerns the reputation of the organization in question (Almaiah et al., 2023; Apau et al., 2025; Cardoso & Cardoso, 2024). Reputation is a corporate resource representing the strategic value of cumulative assessments of credibility, dependability, and ethical responsibility (Farooq et al., 2021; Fombrun, 1996). In the context of Islamic finance, competence, integrity, and other aspects of trust are additionally influenced by religiosity, impacting the evaluation of organizational behaviors and signalling (Muflih et al., 2024; Wahyuni, 2012). Specifically, religiosity not only refers to personal characteristics of customers but also serves as a criterion for assessing whether organizations act in accordance with Islamic principles.

Despite extensive research on trust in digital finance, existing studies predominantly focus on trust formation rather than trust recovery. Prior research highlights the importance of security and privacy in digital banking adoption (Almaiah et al., 2023; Jafri et al., 2024; Susanti et al., 2023), the role of reputation in building credibility and loyalty (Cardoso & Cardoso, 2024; Farooq et al., 2021), and the influence of religiosity on satisfaction and trust in Islamic banking (Muflih et al., 2024; Usman et al., 2017; Wahyuni, 2012). However, limited attention has been given to how these factors interact in crisis situations such as cyber incidents, where trust is disrupted and must be actively rebuilt. This gap indicates the need for an integrated approach that examines both technical and value-based determinants of trust in post-incident contexts. Understanding this interaction is particularly important in Islamic banking, where customer evaluations are shaped by both functional performance and ethical alignment.

Based on this gap, the present study investigates the effects of perceived security, risk management, and reputation on customer trust in Islamic banking following a cyber incident, with religiosity examined as a mediating variable (Almaiah et al., 2023; Cardoso & Cardoso, 2024; Farooq et al., 2021; Fombrun, 1996; Muflih et al., 2024; Susanti et al., 2023). In this context, perceived security and risk management capture aspects such as data protection, transaction safety, and institutional preparedness in responding to cyber threats. The novelty of this study lies in integrating technical, reputational, and socio-religious dimensions within a single framework to explain trust restoration rather than initial trust formation. The findings are expected to contribute to the theoretical development of trust recovery in digital finance and provide practical insights for Islamic banks in managing customer relationships in a digitally vulnerable environment. By linking cyber-related perceptions to post-incident trust, this study offers a more comprehensive understanding of how trust can be rebuilt in Islamic banking.

LITERATURE REVIEW

Organizational Trust Repair as the Theoretical Lens

Since the present study deals with trust recovery after a cyber incident rather than initial trust development, the theory of organizational trust repair serves as a suitable theoretical basis. Organizational trust repair literature discusses how stakeholder trust may be repaired after major failures that destroy organizational legitimacy and harm perceptions of ability, integrity, and benevolence. Such dimensions are very important in the case of cyber incidents when service interruptions are coupled with threats to data security and integrity. According to Gillespie and Dietz (2009), trust repair in organizations involves a multi-step process during which there should be credible indications of regained trustworthiness. In turn, Dirks et al. (2009) outline the most common methods for repairing relationships broken by breaches of trust. Regarding institutions' trust repair efforts, Bachmann et al. (2015) describe main approaches used for that purpose. Moreover, empirical studies reveal the importance of organizational reactions to cyber incidents for trust reconstruction (Kim et al., 2004). Where Islamic banking is concerned, the concept of trust repair goes well beyond technical capability and includes the issue of ethical accountability based on religious values. The assessment of trust takes into consideration not only recovery of effectiveness, but also conformity with the principles of *amānah* and *ʿadālah*, which represent more general *maqāṣid*-based expectations for stakeholder protection (Alwi et al., 2021; Mergaliyev et al., 2021).

Commitment–Trust Theory

Commitment-Trust Theory assumes trust and commitment to be key intermediaries that ensure relational exchanges in uncertain situations (Morgan & Hunt, 1994). In banking, trust plays an important role as a relational resource that ensures service continuity, customer retention, and loyalty. Research findings confirm that communication, reliability, and other relational resources used in relationship marketing significantly impact relational outcomes (Palmatier et al., 2006). Previous research also shows that trust and commitment have different roles within relational exchanges, with trust preceding commitment and both having influence on behavioral intentions of customers (Garbarino & Johnson, 1999). In case of Islamic banking, such relations are additionally affected by ethical norms and beliefs. Customer commitment in this context is formed through observing compliance of institutions to Sharia principles based on such concepts as transparency, fairness, and accountability. Thus, cyber disturbances not only disrupt relations functionally, but they may also imply unethical behavior on

the side of an institution. Such a deterioration in the level of trust leads to a decrease in customer commitment in both practical and ethical terms (Fauzi & Suryani, 2019; Mohsin Butt & Aftab, 2013).

Technology Acceptance Model (TAM)

Technology acceptance model describes how technology behavior is impacted by perceptions of usefulness and ease of use (Davis, 1989), although the model has been extended over time to include social and cognitive factors that affect intention and usage behavior (Venkatesh & Davis, 2000). Trust has been found to be an important element in the digital environment, similar to the elements included in the TAM framework, especially in situations characterized by uncertainties and risk perception (Gefen et al., 2003). Recent studies in integrating the aspects of trust and risk in technology adoption have revealed that while technology acceptance and continuance involve perceived benefits, uncertainty and risk considerations also play a part (Pavlou, 2003). In the case of Islamic digital banking, however, such considerations are further affected by religiosity, through which technological capabilities are evaluated. This means that security and risk mitigation are seen not only as functional requirements but also as ethics-related, as per the tenets of Islam. Research shows that religiosity affects consumer perception of Islamic banking products (e.g., mobile banking applications) as well as trust building (Abou-Youssef et al., 2015; Muflih et al., 2024).

In summary, from these theoretical bases, there are good reasons to be concerned about trust repair in cases where cyber incidents have occurred. The basis of trust repair theory shows the processes through which trust may be restored within the organization in relation to the disruption in the form of communication signalling greater reliability and accountability. Commitment–trust theory focuses on the fact that the restored trust in relation to the disruption in relation to service-oriented interaction would be important in terms of sustaining commitment over the long term. On the other hand, through TAM and its trust and risk-based variations, we can understand the customer's reliance on their security perceptions and risk-related beliefs when they interact within digital banking sites. Drawing from these concepts, the present work sees perceived security and risk management as measures of institutional competence in dealing with cyber-related issues, whereas reputation is seen as an indicator of integrity-based competence. Religious beliefs serve as the evaluative framework here for interpreting these institutional signals in terms of trust.

Cybersecurity in Digital Banking

In today's era, security threats in the field of financial services have resulted in two simultaneous consequences in terms of erosion of trust, one being disruption to operations resulting from loss of service availability and second, breach of data compromise or extortion involving confidentiality and integrity aspects (Reshmi, 2021). Both these factors increase customer uncertainty and perceptions about vulnerability of institutions. On the other hand, the importance of proper post-breach management efforts by companies in terms of communications and response activities in order to cope with customers' needs and manage trust-based consequences of breaches is highlighted by existing studies (Guo et al., 2024). Additionally, findings of empirical studies conducted in banks suggest that perception of cyber risks and security strategies not only impact on the issue of trust but also relational commitment on the part of customers (Bajwa et al., 2023), implying that there is a close connection between behavioral responses of customers and cybersecurity. In an Islamic environment where trust issues relate to ethical legitimacy, the above problem becomes even more complicated.

Perceived Security

Customer perceived security denotes the degree to which customers feel safe in terms of protecting their personal data and transactions against any type of intrusion, fraud, and cyberattacks (Lestari et al., 2024). Indeed, in digital finance, customer perceived security becomes one of the most prominent variables when explaining customer acceptance of new technologies and trust. For example, according to Jafri et al. (2024), security is a prerequisite for FinTech adoption, whereas, in line with Raza et al. (2020), security and privacy become critical components when developing customer trust and loyalty towards using mobile banking services. As evidenced by meta-analysis studies, customer perceived security ranks among the top predictors of mobile banking adoption (Ladeira et al., 2025). Moreover, according to Chong et al. (2021), customer perceptions about the level of security and privacy provided by mobile payment apps significantly influence customer continuance behavior with these services. Finally, according to Bigné et al. (2022), customer perceived security forms a foundational element of digital trust development.

The perception of security in relation to Islamic banking involves more than just a practical function; it also entails consistency with ethical considerations. According to Eid et al. (2020), religiosity positively influences customer assessment when the service offered adheres to Islamic ethics. On a similar line, Islam et al. (2021) state that consumer perceptions of the

institution are influenced by their religiosity, implying that security perception could enhance assessments made in accordance with religious expectations. Hence, not only does the concept of security play an important part in safeguarding customers, but it also signifies institutional accountability. Such significance means that security perceptions could impact trust and religion at the same time. In this regard, it is anticipated that security will affect customer trust in a positive way while improving evaluation made on the basis of religion in Islamic banking.

H1: Perceived security has a positive effect on trust in Islamic banking.

H2: Perceived security has a positive effect on religiosity in Islamic banking.

Risk Management

Risk management can be described as a range of activities performed by organizations to recognize and mitigate threats that have the potential to negatively affect organizational operations or compromise the stakeholders' trust. With the advent of the technological age, cyber threats have become ubiquitous and thus, risk management becomes necessary to ensure financial stability and build the necessary trust among customers (Kaur et al., 2024). For Islamic banks, a systematic approach to risk management contributes to the overall resilience of such institutions while reinforcing trust of their customers (Hossain et al., 2025). At the same time, transparency of information sharing and communication following cyber disruptions are crucial for restoring customer trust in the organization (Ashraf et al., 2023). This claim is confirmed by Khan et al. (2022), who emphasize that justice-based recovery processes including transparency and appropriate risk control and management measures contribute to trust among customers within digital ecosystems. Mahmood et al. (2023) argue that an appropriate response strategy developed by institutions in case of a data breach also affects customers' attitudes towards banking services.

Risk management in the context of Islamic banking involves two aspects: (1) as a functional activity and (2) as an ethical practice that corresponds to the ethical concept of ḥifẓ al-māl. From this standpoint, risk management becomes an ethical obligation and goes beyond the scope of merely being an inevitable process for the bank’s efficient function. It should be noted that according to Apau et al. (2025), risk management plays a positive role in the enhancement of organizational competence perception. Furthermore, as Taneja et al. (2024) emphasize, the perception of risk has a significant effect on the further adoption of mobile banking services. Risk governance and religiosity have a weak connection because risk practices are more related to technical issues for most customers. Nevertheless, risk management practices

that are based on ethical principles may become relevant to religious norms and values influencing religiosity-based perception (Hossain et al., 2025). Hence, risk management is anticipated to have a positive effect on customer trust while providing additional indirect effects as well.

H3: Risk management has a positive effect on trust in Islamic banking.

H4: Risk management has a positive effect on religiosity in Islamic banking.

Reputation

Reputation is an intangible strategic asset that serves to mitigate risk and build client confidence (Fombrun, 1996). The role of reputation in increasing trust, satisfaction, and customer loyalty has been confirmed in the banking sector in situations associated with informational asymmetries (García-Madariaga & Rodríguez-Rivero, 2022). This role takes special significance for Islamic banks because the issues of reputation and credibility are highly correlated with Shariah compliance. Farooq et al. (2021) report that strong Shariah governance is essential for developing reputation and increasing customer trust. Another factor that affects the role of reputation in Islamic banking is the religious affiliation of clients since religion may affect their perception of reputation. According to Usman et al. (2017), religiosity significantly magnifies the impact of reputation on consumer attitudes. Similarly, Gao et al. (2024) state that reputation, which depends on Shariah compliance and cybersecurity capabilities of banks, contributes to building market confidence. In turn, research conducted in the context of digital banking supports the idea that reputation also increases client satisfaction and loyalty (Cardoso & Cardoso, 2024).

H5: Reputation has a positive effect on trust in Islamic banking.

H6: Reputation has a positive effect on religiosity in Islamic banking.

Religiosity and Trust

Religiosity is an essential factor affecting customer satisfaction, loyalty, and trust in Islamic banking institutions (Alrasyid et al., 2023; Muflih et al., 2024; Wahyuni, 2012). The level of religiosity affects how customers perceive their relationship with the institution, which means that their assessment is based on congruence between their religious requirements and those of the institution. According to Eid et al. (2020), religiosity enhances consumers' attitudes regarding Islamic financial institutions by ensuring perceived value congruence. Moreover, Islam et al. (2021) establish that religiosity systematically impacts consumer behavior in the context of Islamic services. Additionally, religiosity can serve as a psychological coping strategy when crises occur. In this case, the customer can consider institutional failures from

an ethical perspective, helping them to retain their faith in the organization despite interruptions in service delivery. Such behavior is vital in post-cyber-attacks since technology issues could affect customers' perceptions of Islamic financial institutions. In summary, besides being a driver of trust formation, religiosity is crucial in recovering lost trust after a crisis.

H7: Religiosity has a positive effect on trust in Islamic banking.

Mediating Role of Religiosity

Religiosity may have effects that go beyond its direct influence, as it also serves as a mediator in shaping consumers' perception of institutional mechanisms. Farooq et al. (2021) indicate that reputation influences customers' trust in institutions through religiosity since their judgment of institution's credibility is based on the alignment of the latter's conduct with Islamic ethics and values. In other words, reputational indicators of institutions are considered not simply in terms of their technical and performance-related nature, but in accordance with religious requirements. Likewise, according to Susanti et al. (2023), security perceptions can affect trust via ethical responsibility and accountability perceptions, which means that security, while being a technical issue, also acquires religious meanings. Similarly, Gao et al. (2024) assert that a combination of cybersecurity with Shariah governance increases confidence, which is rooted both in technical expertise and religion. Thus, one can conclude that the relationship between religiosity and other institutional factors goes beyond mere coexistence and involves mediation, when religious aspects of certain organizational activities shape their interpretation. Consequently, religiosity allows institutional actions to gain moral legitimacy and better promote trust among customers.

H8: Religiosity mediates the relationship between perceived security and trust in Islamic banking.

H9: Religiosity mediates the relationship between risk management and trust in Islamic banking.

H10: Religiosity mediates the relationship between reputation and trust in Islamic banking.

METHOD

In this study, quantitative explanatory research design was used through cross-sectional surveys to explore the effects of the variables, including the perception of security, risk management, reputation, and religiosity as a mediating variable, on the customer trust in Islamic banks. This research design is best suited when dealing with multiple variables and exploring the cause-and-effect relationship at a point in time. Using cross-sectional surveys

makes it possible to collect data from a wide range of participants efficiently while also taking into account their post-cyber incident experiences. This study took place in the Islamic banking context in Indonesia, where the participants were the customers of digital banking services. Such a study setting is ideal considering the current growth in the digital finance industry and the growing cybersecurity risks.

The study targeted the population of Islamic bank customers in Indonesia who actively use digital channels of transaction such as mobile and internet banking. The purposeful sampling approach was employed to select participants who could provide pertinent information concerning the research problem. The following inclusion criteria were considered: (1) customers of Islamic banks in Indonesia; (2) using mobile or internet banking in the previous six months; (3) having age at least 18 years old; and (4) encountering any form of disruption due to cyber issues like service interruptions or limitation in the use of their accounts. Any response that lacked some information was considered incomplete. The number of qualified responses after the filtering process was 247. It surpassed the minimum required number for analysis (Hair et al., 2019; DeSimone et al., 2015).

The data collection process took place in March-May 2025 and entailed completion of an online questionnaire using a five-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree). The use of the online questionnaire, which was sent via e-mail and posted to social media platforms, was facilitated by the support provided by the Indonesian Sharia Fintech Association (AFSI). To develop the questionnaire items, Table 1 presents variable, indicators and instruments.

The data analysis was conducted using Partial Least Square Structural Equation Modelling (PLS-SEM). The data analysis involved a two-step procedure: (1) the measurement model, evaluated reliability and validity, and (2) the structural model, examined the hypotheses testing. For reliability purposes, Cronbach's alpha and composite reliability were computed, while convergent validity was assessed through outer loadings and Average Variance Extracted (AVE). As regards discriminant validity, the Fornell-Larcker criterion and the Heterotrait-Monotrait ratio were used for evaluating it. Furthermore, to test the hypotheses, bootstrapping analysis using 5,000 repetitions was used for estimating the path coefficients and determining their significance level. Effect size (f^2), coefficient of determination (R^2), and predictive relevance (Q^2) were also evaluated to see how good the model worked. The mediating role of religiosity was tested based on the procedure recommended by Zhao et al. (2010).

Table 1. Variable, Indicators, and Instruments

Variable	Indicators	Instruments
Perceived Security (SC)	1. Data Protection 2. Unauthorized Access Prevention 3. Secure Transaction Technology. 4. Security Update Regularity 5. International Security Standard Compliance (Hossain et al., 2025; Jafri et al., 2024; Raza et al., 2020)	1. Security system is trustworthy in protecting my personal data. 2. The system prevents unauthorized access to my account/personal information. 3. The bank uses effective security technology to ensure safe digital transactions. 4. The digital security system is updated regularly. 5. The bank complies with internationally recognized security standards to protect customer data.
Risk Management (MR)	1. Rapid Threat Identification 2. Mitigation Effectiveness 3. Service Recovery Speed 4. Future-Ready Risk Procedures 5. Risk Policy Transparency (Hossain et al., 2025; Jafri et al., 2024; Raza et al., 2020)	1. The bank can identify cyber threats quickly. 2. The bank's mitigation actions effectively reduce the impact of cyberattacks. 3. Digital services are restored quickly and efficiently after a cyber disruption. 4. The bank has professional procedures to manage cyber risks and protect data in the future. 5. The bank provides transparent information about its risk management policies.
Reputation (RP)	1. Sharia Consistency 2. Reputation Resilience 3. Sharia Values Commitment 4. Positive Media Signal 5. Negative Media Impact (Farooq et al., 2021; Madariaga & Rivero, 2022)	1. The bank consistently applies Sharia principles despite challenges. 2. The bank's reputation remains resilient after cyber incidents due to justice-oriented handling. 3. The bank's reputation reflects commitment to Sharia values. 4. Positive media information about the bank's actions increases my confidence. 5. Negative media coverage influences my view of the bank.
Religiosity (RL)	1. Islamic Principal Alignment 2. Sharia Rule Importance 3. Sharia Compliance Belief 4. Riba-Free Assurance 5. Religious Responsibility 6. Religiosity-Driven Continuance (Alrasyid et al., 2023; Islam et al., 2021; Wahyuni, 2012)	1. I prefer Islamic Banking due to its adherence to Islamic guidelines. 2. Adhering to Sharia rules, including in the financial field is important. 3. I believe Islamic banks are truly Sharia-compliant in products and services. 4. Islamic banking gives me the confidence that my transactions are riba-free.

		5. Using Islamic banking is part of my religious responsibility. 6. My religious commitment affects my decision to keep using Islamic banking.
Trust (TR)	1. Consistent Digital Use 2. Digital Reliability 3. Perceived Digital Safety 4. Trust from Service Improvement 5. Long-Term Commitment 6. Recommendation Willingness (Alrasyid et al., 2023; Morgan & Hunt, 1994; Muflih et al., 2024)	1. I use the bank's digital services consistently. 2. The bank's digital services are reliable in securing my data and transactions. 3. I believe the bank's digital services are safe to use. 4. Service improvements increase my trust in the bank's digital services. 5. I am committed to continuing to use the bank in the long term. 6. I am willing to recommend the bank's digital services to others.

Source: Author's Data Processing (2025)

RESULTS

The demographic description of the 247 valid respondents provides us insights into how to interpret the results of this study. There were more females (61.5%) compared to males in the sample, with most of the respondents belonging to age bracket 21-30 years old (77.7%). As for their educational qualifications, senior high school (43.3%) and bachelor degree (40.9%) appeared to be predominant among them. From the occupational perspective, there were more students (55.9%) than any other type of respondents in the sample, followed by entrepreneurs (15.8%) and private sector employees (14.2%). This implies that digital Islamic banking service application is used mainly by young and economically active population. When speaking about the economic status of the population used for analysis, we should mention that more than half of the respondents belonged to low-income families (59.9%). However, despite being in lower income bracket, there were respondents with considerable experience in using digital banks: 38.9% reported having 1-2 years of usage while 32.0% stated that their experience exceeded 2 years. Therefore, in spite of low income, people still have quite extensive experience in using digital banking applications.

Before conducting the statistical assessment of the measurement model, the relationships between indicators and their respective constructs are first presented to provide a clear overview of the reflective measurement structure applied in this study. Figure 1 illustrates the outer (measurement) model, depicting how each indicator is assigned to its corresponding latent construct. By presenting this visual overview, the study ensures greater transparency in

how the measurement framework is specified prior to formal evaluation. In addition, the outer model serves as a conceptual guide for interpreting the subsequent results of reliability and validity testing. Overall, this visualization facilitates a clearer understanding of the measurement structure and supports the interpretation of the statistical analyses reported in Tables 2–4.

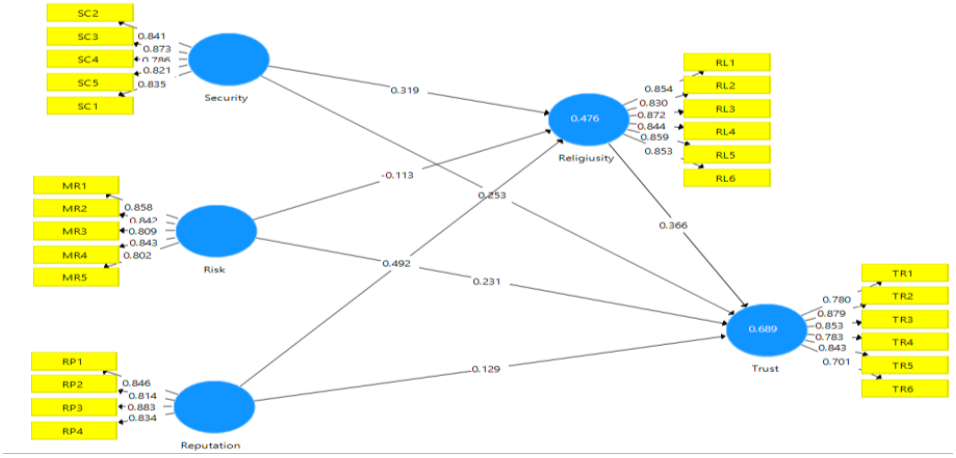

Figure 1. Final PLS-SEM Structural Model
Source: Author's data processing (2025)

Measurement Model Results

Before carrying out the analysis of the structural model, the measurement model was assessed to ascertain whether all constructs were adhering to the standards of reliability and validity. From Table 2, it is clear that all indicators obtained outer loading scores greater than the recommended cut-off point of 0.70, with values varying between 0.701 and 0.883, which implies sufficient indicator reliability (Hair et al., 2019). All trust indicators (TR1 to TR6) obtained scores varying between 0.701 and 0.879, but only TR6 was acceptable even though it exhibited a lower score. Religiosity indicators (RL1 to RL6) obtained very high loading scores between 0.830 and 0.872, while those of reputation (RP1 to RP4), security (SC1 to SC5), and risk management (MR1 to MR5) were also relatively high. Cronbach's alpha scores varied between 0.866 and 0.925, all being greater than the minimum threshold of 0.70, and all composite reliability scores were greater than 0.90, showing sufficient internal consistency.

Discriminant validity was assessed using the Fornell–Larcker criterion and the HTMT. In Table 3, the square roots of the AVE (diagonal values) were greater than the correlations between constructs, confirming that each construct is empirically distinct. Furthermore, Table 4 presents the HTMT ratios, all below the threshold of 0.90, with the highest being 0.878 (reputation–security). This further confirms discriminant validity.

Table 2. Measurement Model Results

Construct	Item	Outer Loading	Cronbach's Alpha	Composite Reliability	AVE
Religiosity	RL1	0.854	0.925	0.941	0.726
	RL2	0.830			
	RL3	0.872			
	RL4	0.844			
	RL5	0.859			
	RL6	0.853			
Reputation	RP1	0.846	0.866	0.909	0.713
	RP2	0.814			
	RP3	0.883			
	RP4	0.834			
Risk Management	MR1	0.858	0.888	0.918	0.691
	MR2	0.842			
	MR3	0.809			
	MR4	0.843			
	MR5	0.802			
Security	SC1	0.835	0.888	0.918	0.692
	SC2	0.841			
	SC3	0.873			
	SC4	0.786			
	SC5	0.821			
Trust	TR1	0.780	0.893	0.918	0.654
	TR2	0.879			
	TR3	0.853			
	TR4	0.783			
	TR5	0.843			
	TR6	0.701			

Source: Author's Data Processing (2025)

Table 3. Fornell–Larcker Criterion

Construct	Religiosity	Reputation	Risk	Security	Trust
Religiosity	**0.852**				
Reputation	0.663	**0.844**			
Risk	0.430	0.663	**0.831**		
Security	0.622	0.772	0.680	**0.832**	
Trust	0.709	0.721	0.646	0.738	**0.808**

Source: Author's Data Processing (2025)

Table 4. HTMT Ratio

Construct	Religiosity	Reputation	Risk	Security	Trust
Reputation	0.739				
Risk	0.473	0.754			
Security	0.684	0.878	0.765		
Trust	0.772	0.815	0.727	0.822	

Source: Author's Data Processing (2025)

Structural Model Results

According to the results displayed in Table 5 below, the model shows considerable explanatory power in relation to endogenous variables. Perceived security, risk management, and reputation account for 47.6% of the variance of religiosity (R^2 = 0.476; adjusted R^2 = 0.470). Hence, the model reveals moderate explanatory power and implies that these antecedents have a significant effect on shaping evaluations based on religiosity within the domain of Islamic banking. In addition, 68.9% of the variance of trust (R^2 = 0.689; adjusted R^2 = 0.684) is explained by this model, which signifies great accuracy, taking into consideration established criteria of predictive power (Hair et al., 2022). Therefore, a rather significant proportion of the variation of trust can be attributed to perceived security, risk management, reputation, and religiosity. Thus, these results imply that the developed theoretical framework has satisfactory predictive ability and is appropriate for investigating relationships among technical, reputational, and value-based factors affecting trust development in Islamic digital banking.

Effect sizes were calculated to assess the relative contribution of each exogenous construct to the endogenous variables. As shown in Table 6, religiosity demonstrates a moderate effect on trust (f^2 = 0.226), indicating its substantial role in shaping customer trust within the model. Reputation shows a meaningful effect on religiosity (f^2 = 0.170), suggesting that perceptions of institutional credibility significantly influence religiously grounded evaluations. Perceived security exhibits a small but notable effect on both religiosity (f^2 = 0.069) and trust (f^2 = 0.068), indicating that security perceptions contribute modestly to both constructs. Risk management shows a small effect on trust (f^2 = 0.083), but its effect on religiosity is minimal (f^2 = 0.012), implying a limited role in shaping value-based perceptions. In contrast, reputation has only a trivial direct effect on trust (f^2 = 0.017), reinforcing the idea that its influence operates primarily through religiosity rather than directly affecting trust.

The predictive relevance of the model was tested through the blindfolding technique, which tests the out-of-sample predictive ability of the model. As can be seen in Table 7, the endogenous constructs both have Q^2 scores above zero (Religiosity = 0.341; Trust = 0.444). Therefore, we conclude that the model demonstrates sufficient predictive relevance, i.e., it can predict the observed sample without being just a good fit. Moreover, the higher Q^2 score of trust is associated with better predictive power for the important construct under study. Thus, we find confirmation in this case that the developed model is both statistically strong and practically relevant.

Table 5. Coefficient of Determination (R^2)

Construct	R^2	Adjusted R^2	Interpretation
Religiosity	0.476	0.470	Moderate
Trust	0.689	0.684	Substantial

Source: Author's Data Processing (2025)

Table 6. Effect Sizes (f^2)

Path	f^2	Interpretation
Religiosity → Trust	0.226	Medium
Reputation → Religiosity	0.170	Medium
Risk → Religiosity	0.012	Negligible
Risk → Trust	0.083	Small
Security → Religiosity	0.069	Small
Security → Trust	0.068	Small
Reputation → Trust	0.017	Negligible

Source: Author's Data Processing (2025)

Table 7. Predictive Relevance (Q^2)

Construct	Q^2	Interpretation
Religiosity	0.341	Medium
Trust	0.444	Large

Source: Author's Data Processing (2025)

Path Coefficients and Mediation Analysis

The significance of the hypothesized relationships was assessed using a bootstrapping procedure. Table 8 shows the results provide partial support for the proposed hypotheses. Religiosity shows a significant positive effect on trust. Reputation significantly influences religiosity, but does not have a direct effect on trust, suggesting that its impact operates indirectly through value-based evaluations. Risk management has a significant direct effect on trust, yet its influence on religiosity is not significant, indicating that customers primarily interpret risk practices as technical rather than value-driven. In contrast, perceived security significantly affects both religiosity and trust, highlighting its dual role as both a functional and value-relevant factor.

The mediating effect of religiosity was shows in Table 9, reputation exhibits a significant indirect effect on trust mediated by religiosity, which implies full mediation since the direct effect of reputation on trust is insignificant. Likewise, perceived security exhibits a significant indirect effect on trust mediated by religiosity, implying partial mediation since security also has a direct impact on trust besides its indirect effect mediated by values. On the other hand, there is no significant indirect effect of risk management on trust mediated by religiosity.

The findings confirm that customer trust in Islamic banking is shaped by both technical and ethical considerations. Religiosity emerges as the strongest predictor of trust, functioning not only as a direct determinant but also as a mediating mechanism that links institutional factors to trust outcomes. Reputation influences trust only indirectly through religiosity, indicating that customers interpret reputational signals within the framework of their religious values rather than as purely objective indicators of credibility. Perceived security demonstrates both direct and indirect effects on trust, highlighting its dual role as a source of practical assurance and as a signal of alignment with ethical and religious expectations. In contrast, risk management exerts a significant direct effect on trust but does not significantly influence religiosity, suggesting that customers primarily perceive it as a technical capability rather than a value-driven practice. Overall, these results emphasize the importance of integrating technological competence with ethical alignment to effectively build and sustain trust in Islamic banking contexts.

Table 8. Path Coefficients (Direct Effects)

Path	β	t-value	p-value	Result
Religiosity → Trust	0.366	2.624	0.009	Supported
Reputation → Religiosity	0.492	5.169	0.000	Supported
Reputation → Trust	0.129	1.095	0.274	Not Supported
Risk → Religiosity	–0.113	1.632	0.103	Not Supported
Risk → Trust	0.231	4.567	0.000	Supported
Security → Religiosity	0.319	3.405	0.001	Supported
Security → Trust	0.253	2.756	0.006	Supported

Source: Author's data processing (2025)

Table 9. Mediation Effects via Religiosity

Indirect Path	β	t-value	p-value	Mediation Result
Reputation → Religiosity → Trust	0.180	2.644	0.008	Supported (Full)
Risk → Religiosity → Trust	–0.041	1.317	0.188	Not Supported
Security → Religiosity → Trust	0.117	2.146	0.032	Supported (Partial)

Source: Author's data processing (2025)

DISCUSSION

The Effect of Perceived Security, Risk Management, And Reputation on Trust in Islamic Banking

Perceived security positively impacts customer trust in Islamic banks after any cyber-based disruption. This aligns with contemporary cybersecurity threats faced by financial services where any disruption is likely

to lead to worries regarding the confidentiality and integrity of their transactions. In this regard, customers depend heavily on security assurance for regaining lost confidence. As per the theory of trust repair, perceived security operates as a competence cue to lower vulnerability and restore customers' trust. Similarly, the use of security cues to reduce uncertainties related to technology-mediated transactions supports the perspective of technology-related trust. Considering the demographic profile comprised predominantly of young and active internet users, perceived security continues to be relevant due to regular experiences with mobile banking, thus becoming a prominent trust restorer. This conclusion corroborates with existing findings that security perception is one of the key determinants of online trust and intention to continue usage in banks and fintech firms (Chong et al., 2021; Jafri et al., 2024; Raza et al., 2020).

Moreover, the role of risk management enhances the trust factor because it seems that the consumers appreciate the organization's readiness and ability to mitigate any risks and provide recovery from possible service disruptions caused by any cyber incidents. It corresponds to modern cyber trends within the financial industry, as banks' activities have been evaluated not just on the effectiveness of their preventive measures but also on how successfully they cope with any disruption and ensure service continuity. As per the trust repair theory, corrective actions and control improvements are essential instruments for repairing ability-based trust, and hence, the perception of risk management serves as a practical indicator of the bank's capability in managing any cyber risks. The fact that the participants often engage in online banking means that the issue is directly related to their day-to-day activities, which further supports the trust effect.

Reputation does not significantly influence trust in the post-cyber-attack scenario, meaning that reputation perception itself is inadequate in restoring trust immediately following the incident. This is a reflection of reality in cyber world, where after any such events, it is essential for customers to have tangible evidence of safety and continuity of operations as opposed to good reputation or credible history. According to the trust repair theory, post-violation trust relies on credible repairing efforts (such as corrective actions and increased security measures). Moreover, for individuals who use online systems frequently, judgments about trust are likely influenced by actual personal experience with system performance and reliability, thus weakening the link between reputation and trust. Reputation has been found to have a high correlation with trust in financial services (Bajwa et al., 2023; Fombrun, 1996; Madariaga & Rivero, 2022); however, the findings of this study indicate

the need to verify value-based reputation to make it relevant to trust in Islamic banking institutions.

The Effect of Perceived Security, Risk Management, And Reputation on Religiosity in Islamic Banking

Religiosity was found to have a strong correlation with perceived security, implying that customers perceive security as not merely a technical feature, but also as a reflection of ethics and integrity on the part of Islamic banks. In the cyber aftermath, customers assess whether the bank serves as a physical and moral shield to them from dangers such as breaches of security or mishandling of transactions. In terms of trust repair theory, repair occurs more effectively when the institution addresses issues regarding both competence and integrity/benevolence; hence, security measures in Islamic banking can be seen as a form of *amānah* and *ḥifẓ al-māl* in the sense that they provide integrity and safety for their funds and data. Since most of the respondents use digital platforms frequently, security becomes an important attribute which could help the bank to be evaluated from a religiosity perspective (Eid et al., 2020; Islam et al., 2021).

The connection between risk management and religiosity is not statistically significant, suggesting that customers perceive risk management as a capacity-related aspect rather than as an indicator with religious significance. In the case of cyber threats, risk management is evaluated based on concrete results obtained from responses in operations that fix the ability-based perception of trust without making any attempt at value-based religious assessment. This study's findings can be understood using the concept of trust repair, which states that ability repair will only lead to integrity repair when the response is moral responsibility based. As the current study's sample includes mostly technologically-oriented young people, risk management assessments can continue to be operational and pragmatic without necessarily triggering religious considerations, especially if institutional communication follows operational terminology. Such a situation mirrors previous findings, where risk management within Islamic banking was found to be communicated operationally, and its religious implications remained limited unless connected to Islamic ethics (Hossain et al., 2025).

Reputation significantly predicts religiosity, implying that reputational judgments in Islamic banking are closely tied to perceived Sharia alignment and moral credibility. In cyber incidents, stakeholders evaluate not only competence but also ethical integrity and justice in crisis handling; therefore, reputational cues become meaningful when customers interpret them as evidence of principled conduct. Under the theory of trust repair, integrity-

based repair calls for signals that the organisation is still ethically on course. In Islamic banking, reputation can serve as a proxy for perceived Sharia governance and ethical consistency, thereby strengthening religiosity as an evaluative lens. When looking at the characteristics of the respondent, it is observed that those who are digital users continuously get exposed to information flows (service updates as well as media stories). This helps in producing a reputational evaluation and a reinforcement of judgment based on religiosity. This finding is in line with past Islamic banking studies, which assert that Sharia governance augments reputational credibility and that religiosity enhances the reputation's impact on customer attitudes (Farooq et al., 2021; Usman et al., 2017).

The Effect of Religiosity on Trust and The Mediating Role in Islamic Banking

Religiosity greatly boosts trust levels, which suggests that trust restoration in Islamic banking depends on both the technical and moral side of things. In the present-day cyberspace era, events might lead to the loss of legitimacy. In such circumstances, religiosity may play an important role in ensuring trust because customers will be convinced that despite facing the challenges of cybersecurity, the bank still adheres to Islam. In terms of trust repair theory, this indicates that integrity and benevolence restoration occur; customers will be more inclined to give their trust back once they realize that the bank assumes its ethical obligation and Sharia-compliant management. The findings are also consistent with Commitment-Trust Theory where trust serves to preserve the relationship, and religiosity reinforces the perception of legitimacy regarding sustaining the relationship post-disruption. Considering the nature of the respondents who are technologically savvy, religiosity can function as a mental filter for interpreting matters related to security, reputation, and crises (Alrasyid et al., 2023; Eid et al., 2020; Muflih et al., 2024; Wahyuni, 2012).

The utmost outcome of the mediation results shows that perceived security can influence trust mediated by religiosity. In other words, it directly strengthens trust. It is similar to how a cyber incident damages trust: customers need immediate technical reassurance (that transactions are secured and data protected) and also assess if protective effort reflects Islamic ethical responsibility. According to Trust repair theory, security can be viewed as an ability-based repair signal while due to their legitimacy, religiosity can also be viewed as the integrity-based repair signal. Similarly, bank's conduct is justified as *amānah* or stewardship (*ḥifẓ al-māl*). According to those who use digital services often, a direct pathway reflects actual usage of secure banking,

while an indirect pathway reflects consumer confidence that the bank is ethically responsible in safeguarding customers. This trend is consistent with digital trust research, which underlines the direct role of security, and Islamic service research, which emphasizes religiosity as an interpretive mechanism (Eid et al., 2020; Islam et al., 2021; Jafri et al., 2024; Raza et al., 2020).

Religiosity acts as neither mediator nor moderator in the association between risk management and trust, meaning that risk governance increases trust predominantly via a technical pathway, as opposed to a value pathway. The efficacy of risk management in cyber-attacks is determined based on pragmatic criteria including effectiveness of risk mitigation and speed of recovery of services provided, thus facilitating the process of rebuilding trust based on competence. According to trust repair theories, technical interventions may restore ability-based trust irrespective of whether or not there is an impact on integrity-based trust unless the former is seen as ethical accountability; this explains the lack of mediation in the current case. The high digital activities of respondents imply that risk management is assessed purely operationally and on the basis of performance, instead of being viewed from the perspective of its Sharia values (Hossain et al., 2025).

Reputation's impact on trust is fully mediated by religiosity, such that reputation increases trust only through its effect on evaluation according to religiosity. This captures the post-cyber-incident environment where consumers do not increase their level of trust merely because of the reputation of the service provider but do so if the reputation triggers the perception that the provider adheres to the requirements of Sharia law, justice, and ethical values. The theoretical framework on trust repair highlights the significance of restoring integrity following violations; in Islamic banking, religiosity is the process by which reputational information is validated as morally correct and hence relevant to trust building. For heavy users of the Internet familiar with the crisis narrative, information about reputation is evaluated for its ethical correctness within religion before being transformed into trust recovery (Farooq et al., 2021; Usman et al., 2017).

Integrative Implication for Cyber Context and Theoretical Contribution

As such, the results reveal that post-incident trust in Islamic digital banking is dependent on competency cues like security and recoverability, while reputation cues only lead to trust when backed by religious validation. These results are congruent with trust restoration theory, where trust is restored not from initial perceptions, but instead from visible indicators and responses to failures after an organizational-level incident occurs (Aisyah et al., 2025). The results are also supported by literature regarding data

breaches, which highlights that disclosure and restoration activities play a critical role in shaping customer trust post-incident (Muzatko & Bansal, 2024).

Overall, the results suggest that for Islamic digital banking to foster successful cyber resilience, it is necessary to combine competency-based trust cues with integrity based on religious validation, specifically among highly digitally engaged consumers. In this regard, this study has enhanced the theoretical knowledge base regarding the restoration of post-incident trust in Sharia-compliant digital banking by combining trust repair theory, commitment-trust theory, and TAM (Eid et al., 2020; Farooq et al., 2021; Hossain et al., 2025).

CONCLUSION

The current study attempted to identify the role of security perception, risk management, reputation, and religiosity on the rebuilding of customer trust in Islamic banks after cyber-attacks. According to the results, the rebuilding process relies on the interaction between the technical and value-based factors of trust. More specifically, security perception and risk management emerge as two important technical factors of trust, while security perception also positively affects religiosity. Thus, technological aspects are linked to value perception in the context of building trust relationships. At the same time, reputation does not have a direct effect on trust, but only through religiosity, which indicates the interpretation of institutional credibility via religious considerations during critical incidents. Hence, religiosity becomes both a direct and indirect factor of trust. In particular, from the theoretical perspective, Commitment-Trust theory can be further extended to the specific domain of Islamic digital banking, taking into account that apart from competence and relational aspects, the process of trust is also associated with religiosity, which can be considered a factor of value evaluation.

In terms of managerial implications, the results indicate that Islamic financial institutions need to improve their cybersecurity infrastructure and risk management practices in an ethical manner that aligns with Shariah. Effective communication about cybersecurity and recovery activities should highlight the themes of accountability, transparency, and the need to protect the interest of stakeholders. Reputation management for Islamic banks needs to be built on ethics, since the signal of religiosity seems to play an important role in transforming reputation into trust. As risk management messages do not inherently carry the connotation of religiousness, banks could incorporate values into their communications to make themselves morally responsible and trustworthy. The participation of stakeholders who have high legitimacy among the public can also help build trust quickly. The limitations of the study

include the use of self-report surveys, a cross-sectional design that prevents causal analysis, and the use of Indonesian samples. To extend the present research to other contexts, researchers are encouraged to adopt longitudinal research designs, expand cross-country studies, and adopt qualitative methods to explore customer perceptions in different countries regarding how Islamic banks should communicate about cybersecurity issues and recovery activities.

REFERENCES

Abou-Youssef, M. M. H., Kortam, W., Abou-Aish, E., & El-Bassiouny, N. (2015). Effects of religiosity on consumer attitudes toward Islamic banking in Egypt. *International Journal of Bank Marketing*, *33*(6), 786–807. https://doi.org/10.1108/IJBM-02-2015-0024

Aisyah, M., Sesunan, Y. S., & Wicaksono, A. T. S. (2025). Customers' trust in Islamic banking post-cyberattack leads to digital service breakdowns in Indonesia. *Sustainable Futures*, *10*, 101530. https://doi.org/10.1016/j.sftr.2025.101530

Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the Role of Perceived Risk, Perceived Security and Perceived Trust on Smart m-Banking Application Using SEM. *Sustainability*, *15*(13), 9908. https://doi.org/10.3390/su15139908

Alrasyid, H., Rabbani, M. R., & Afifudin. (2023). *Embracing the digital economy : Exploring the role of trust , perceived ease of use , and religiosity on intention to use Islamic peer-to-peer lending*. *20*(2), 283–305. https://doi.org/10.31106/jema.v20i2.9097

Alwi, Z., Parmitasari, R. D. A., & Syariati, A. (2021). An assessment on Islamic banking ethics through some salient points in the prophetic tradition. *Heliyon*, *7*(5), e07103. https://doi.org/10.1016/j.heliyon.2021.e07103

Apau, R., Titis, E., & Lallie, H. S. (2025). Towards a better understanding of mobile banking app adoption and use: Integrating security, risk, and trust into UTAUT2. *Computers*, *14*(4), 144. https://doi.org/10.3390/computers14040144

Ashraf, R., Sharma, P., & Menon, A. (2023). When service recovery meets cyber incidents: Transparency, apology, and assurance in rebuilding trust. *Journal of Service Research*, *26*(4), 566–584. https://doi.org/10.1177/10946705231158728

Bachmann, R., Gillespie, N., & Priem, R. (2015). Repairing Trust in Organizations and Institutions: Toward a Conceptual Framework. *Organization Studies*, *36*(9), 1123–1142. https://doi.org/10.1177/0170840615599334

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. *Information and*

Computer Security, *31*(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179

Bigné, E., Andreu, L., & Hernandez, B. (2022). Digital trust in financial services: Antecedents and outcomes. *Journal of Business Research*, *145*, 1–12. https://doi.org/10.1016/j.jbusres.2022.02.045

Cardoso, A., & Cardoso, M. (2024). Bank Reputation and Trust: Impact on Client Satisfaction and Loyalty for Portuguese Clients. *Journal of Risk and Financial Management*, *17*(7), 277. https://doi.org/10.3390/jrfm17070277

Chong, A. Y. L., Bao, H., & Ooi, K. B. (2021). Cybersecurity, privacy concerns, and continuance intention for mobile payments. *Decision Support Systems*, *141*, 113448. https://doi.org/10.1016/j.dss.2020.113448

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

DeSimone, J. A., Harms, P. D., & DeSimone, A. J. (2015). Best practice recommendations for data screening. *Journal of Organizational Behavior*, *36*(2), 171–181. https://doi.org/10.1002/job.1962

Dirks, K. T., Lewicki, R. J., & Zaheer, A. (2009). Reparing Relationships Within and Between Organizations: Building A Conceptual Foundation. *Academy of Management Review*, *34*(1), 68–84. https://doi.org/10.5465/amr.2009.35713285

Eid, R., El-Gohary, H., & Armesh, H. (2020). Muslim consumers' religiosity and Islamic banking selection: Trust and value congruence perspectives. *Journal of Islamic Marketing*, *11*(4), 1009–1027. https://doi.org/10.1108/JIMA-01-2018-0014

Elansari, H., Alzubi, A., & Khadem, A. (2024). The Impact of United Nations Sustainable Development Goals on Customers' Perceptions and Loyalty in the Banking Sector: A Multi-Mediation Approach. *Sustainability*, *16*(18), 8276. https://doi.org/10.3390/su16188276

Farooq, M., Raza, S. A., & Khan, N. A. (2021). The impact of shariah governance on reputation and trust in Islamic banks. *International Journal of Islamic and Middle Eastern Finance and Management*, *14*(3), 467–485. https://doi.org/10.1108/IMEFM-09-2019-0405

Fauzi, A. A., & Suryani, T. (2019). Measuring the effects of service quality by using CARTER model towards customer satisfaction, trust and loyalty in Indonesian Islamic banking. *Journal of Islamic Marketing*, *10*(1), 269–289. https://doi.org/10.1108/JIMA-04-2017-0048

Fombrun, C. J. (1996). *Reputation: Realizing value from the corporate image*. Harvard Business School Press.

Gao, Y., Waheed, A., & Hassan, M. K. (2024). Shariah governance, cybersecurity capability, and market confidence in Islamic banks. *Pacific-Basin Finance Journal*, *83*, 102176. https://doi.org/10.1016/j.pacfin.2024.102176

Garbarino, E., & Johnson, M. S. (1999). The Different Roles of Satisfaction, Trust, and Commitment in Customer Relationships. *Journal of Marketing*, *63*(2), 70–87. https://doi.org/10.1177/002224299906300205

García-Madariaga, J., & Rodríguez-Rivero, A. (2022). Corporate reputation in banking: Systematic review and research agenda. *International Journal of Bank Marketing*, *40*(7), 1441–1464. https://doi.org/10.1108/IJBM-06-2021-0290

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51–90. https://doi.org/10.2307/30036519

Gillespie, N., & Dietz, G. (2009). Trust Repair After An Organization-Level Failure. *Academy of Management Review*, *34*(1), 127–145. https://doi.org/10.5465/amr.2009.35713319

Guo, Y., Wang, C., & Chen, X. (2024). Functional or financial remedies? The effectiveness of recovery strategies after a data breach. *Journal of Enterprise Information Management*, *37*(1), 148–169. https://doi.org/10.1108/JEIM-10-2022-0372

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2019). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (3rd ed.). Sage.

Hossain, M. A., Rosman, R., Jahan, N., Afroz, S., & Afroza, K. (2025). A Systematic Literature Review of Risk Management in the Islamic Banking System: Research Agenda and Future Directions. *International Journal of Research and Innovation in Social Science*, *IX*(III), 1193–1209. https://doi.org/10.47772/IJRISS.2025.90300093

Islam, T., Ali, G., & Sheikh, Z. (2021). Religiosity and consumer behavior in Islamic services: A meta-synthesis. *Journal of Islamic Marketing*, *12*(5), 909–936. https://doi.org/10.1108/JIMA-09-2019-0186

Jafri, J. A., Amin, S. I. M., Abdul Rahman, A., & Nor, S. M. (2024). A systematic literature review of the role of trust and security on FinTech adoption in banking. *Heliyon*, *10*(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e22980

Kaur, J., Hasan, S. N., Orthi, S. M, Miah, M. A., Goffer, M. A., Barikdar, C. R. & Hassan, J. (2024). Advanced Cyber Threats and Cybersecurity Innovation - Strategic Approaches and Emerging Solutions. *Journal of Computer Science and Technology Studies*, *5*(3), 112–121. https://doi.org/10.32996/jcsts.2023.5.3.9

Khan, I., Hollebeek, L. D., & Ranaweera, C. (2022). Service failure in digital finance and the role of recovery justice and security assurance. *Journal of Service Management*, *33*(6), 1031–1053. https://doi.org/10.1108/JOSM-08-2021-0300

Kholis, I. M. (2025). Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*. https://doi.org/10.14421/t5sfe747

Kim, P. H., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. (2004). Removing the Shadow of Suspicion: The Effects of Apology Versus Denial for Repairing

Competence- Versus Integrity-Based Trust Violations. *Journal of Applied Psychology*, *89*(1), 104–118. https://doi.org/10.1037/0021-9010.89.1.104

Ladeira, J, W., Hasan Jafar, S., & de Oliveira Santini, F. (2025). A meta-analysis of technological adoption of financial services: investigating risk and trust perception effects. *International Journal of Bank Marketing*, 1–29. https://doi.org/10.1108/IJBM-02-2025-0156

Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. *Safer Communities*, *23*(4), 444–464. https://doi.org/10.1108/SC-04-2024-0018

Mahmood, A., Fatima, T., & Khan, M. (2023). Rebuilding customer trust after data breaches in banking. *Electronic Commerce Research and Applications*, *58*, 101233. https://doi.org/10.1016/j.elerap.2023.101233

Mergaliyev, A., Asutay, M., Avdukic, A., & Karbhari, Y. (2021). Higher Ethical Objective (Maqasid al-Shari'ah) Augmented Framework for Islamic Banks: Assessing Ethical Performance and Exploring Its Determinants. *Journal of Business Ethics*, *170*(4), 797–834. https://doi.org/10.1007/s10551-019-04331-4

Mohsin Butt, M., & Aftab, M. (2013). Incorporating attitude towards Halal banking in an integrated service quality, satisfaction, trust and loyalty model in online Islamic banking context. *International Journal of Bank Marketing*, *31*(1), 6–23. https://doi.org/10.1108/02652321311292029

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, *58*(3), 20–38. https://doi.org/10.1177/002224299405800302

Muflih, M., Zen, M., Purbayati, R., Kristianingsih, K., Karnawati, H., Iswanto, B., & Juniwati, E. H. (2024). Customer loyalty to Islamic mobile banking: Evaluating the roles of justice theory, religiosity, satisfaction and trust. *International Journal of Bank Marketing*, *42*(3), 571–595. https://doi.org/10.1108/IJBM-07-2022-0352

Muzatko, S., & Bansal, G. (2024). It pays to be forthcoming: timing of data breach announcement, trust violation, and trust restoration. *Internet Research*, *34*(5), 1629–1663. https://doi.org/10.1108/INTR-12-2021-0939

OJK. (2023, May 13). *BANK SYARIAH INDONESIA OPERATES BACK TO NORMAL, PUBLIC CAN REST ASSURED*. https://ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Pages/Bank-Syariah-Indonesia-Operates-Back-To-Normal%2C-Public-Can-Rest-Assured.aspx?utm_source=chatgpt.com

Palmatier, R. W., Dant, R. P., Grewal, D., & Evans, K. R. (2006). Factors Influencing the Effectiveness of Relationship Marketing: A Meta-Analysis. *Journal of Marketing*, *70*(4), 136–153. https://doi.org/10.1509/jmkg.70.4.136

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model.

International Journal of Electronic Commerce, *7*(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Ramadhanu, T. I., Tanjung, S., Yunus, H., Ahir, H., & Nurbaiti. (2025). Strategi Penguatan Database Nasabah Pada Perbankan Syariah. *JPSDa: Jurnal Perbankan Syariah Darussalam*. https://doi.org/10.30739/jpsda.v5i1.3581

Raza, S. A., Umer, A., & Qazi, W. (2020). Security and privacy as antecedents of trust and usage of mobile banking. *Telematics and Informatics*, *50*, 101118. https://doi.org/10.1016/j.tele.2020.101118

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Shehab, R., S.alismail, A., Amin Almaiah, Dr. M., Alkhdour, Dr. T., AlWadi, Dr. B. M., & Alrawad, Dr. M. (2024). Assessment of Cybersecurity Risks and threats on Banking and Financial Services. *Journal of Internet Services and Information Security*, *14*(3), 167–190. https://doi.org/10.58346/JISIS.2024.I3.010

Sulubara, S. M. (2024). Perlindungan Data Pribadi dalam Kasus Ransomware: Apa Kata Hukum? *Eksekusi : Jurnal Ilmu Hukum Dan Administrasi Negara*. https://doi.org/10.55606/eksekusi.v2i4.1823

Susanti, R., Fitri, F., & Yusuf, A. (2023). Security perception and mobile banking adoption: Evidence from Indonesia. *Sustainability*, *15*(5), 4172. https://doi.org/10.3390/su15054172

Taneja, S., Arora, R., & Dhir, A. (2024). Determinants of mobile banking continuance: Integrating perceived risk, security, and habit. *Computers in Human Behavior*, *149*, 107197. https://doi.org/10.1016/j.chb.2023.107197

Usman, H., Tjiptoherijanto, P., Balqiah, T. E., & Agung, I. G. N. (2017). The role of religious norms, trust, importance of attributes and information sources in the relationship between religiosity and selection of the Islamic bank. *Journal of Islamic Marketing*, *8*(2), 158–186. https://doi.org/10.1108/JIMA-01-2015-0004

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Wahyuni, S. (2012). Moslem religiosity scale: Construct development and validation. *Journal of Islamic Marketing*, *3*(4), 355–371. https://doi.org/10.1108/17590831211281996

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, *37*(2), 197–206. https://doi.org/10.1086/651257

Zouari, G., & Abdelhedi, M. (2021). Customer satisfaction in the digital era: evidence from Islamic banking. *Journal of Innovation and Entrepreneurship*, *10*(1), 9. https://doi.org/10.1186/s13731-021-00151-x